AMENDMENTS TO THE CLAIMS

Please cancel claims 1-26, and add new claims 27-35, such that the status of the claims is as follows:

1-26. (Canceled)

27. (New) A method for providing computer application security, the method comprising:

identifying secured resources within a software application;

grouping secured resources into user roles stored on data stores of a plurality of security brokers, wherein grouping secured resources into user roles comprises:

establishing in the data stores links to each of the secured resources;

selecting the links corresponding to related secured resources;

grouping the selected links into user roles; and

storing the user roles in the data stores;

generating a plurality of surrogate identifiers in the data stores of the security brokers, each surrogate identifier being associated with one user role;

associating users with user roles, each user being associated with one user role; and

determining access rights to the secured resources for each user according to a corresponding surrogate identifier without disclosing the corresponding surrogate identifier to the user, the corresponding surrogate identifier being associated with the user role of the user, determining access rights further comprising:

receiving a permissions request from a workstation and routing the permissions request to one of a plurality of security providers with one of the security brokers;

authenticating a computer user as a valid user with one of the security providers; and

authorizing the user to access one of the secured resources with one of a plurality of security providers.

28. (New) A method for providing computer application security, the method comprising:

identifying secured resources within a software application;

grouping secured resources into user roles stored on data stores of a plurality of security brokers, wherein grouping secured resources into user roles comprises:

establishing in the data stores links to each of the secured resources within the software application;

selecting the links corresponding to related secured resources;

grouping the selected links into privilege sets;

grouping privilege sets and links into user roles; and

storing the user roles in the data stores;

generating a plurality of surrogate identifiers in the data stores of the security brokers, each surrogate identifier being associated with one user role;

associating users with user roles, each user being associated with one user role; and

determining access rights to the secured resources for each user according to a corresponding surrogate identifier without disclosing the corresponding surrogate identifier to the user, the corresponding surrogate identifier being associated with the user role of the user, determining access rights further comprising:

receiving a permissions request from a workstation and routing the permissions request to one of a plurality of security providers with one of the security brokers;

authenticating a computer user as a valid user with one of the security providers; and

authorizing the user to access one of the secured resources with one of a plurality of security providers.

29. (New) A method for providing computer application security, the method comprising:

identifying secured resources within a software application;

grouping secured resources into user roles stored on data stores of a plurality of security brokers, wherein grouping secured resources into user roles comprises:

establishing in the data stores links to each of the secured resources within the software application;

selecting the links corresponding to related secured resources;

grouping the selected links into privilege sets;

grouping privilege sets and links into job functions;

grouping job functions, privilege sets and links into user roles;

and storing the user roles in the data stores;

generating a plurality of surrogate identifiers in the data stores of the security brokers, each surrogate identifier being associated with one user role;

associating users with user roles, each user being associated with one user role; and

determining access rights to the secured resources for each user according to a corresponding surrogate identifier without disclosing the corresponding surrogate identifier to the user, the corresponding surrogate identifier being associated with the user role of the user, determining access rights further comprising:

receiving a permissions request from a workstation and routing the permissions request to one of a plurality of security providers with one of the security brokers;

authenticating a computer user as a valid user with one of the security providers; and

authorizing the user to access one of the secured resources with one of a plurality of security providers.

30. (New) A method for providing computer application security, the method comprising:

identifying secured resources within a software application;

grouping secured resources into user roles stored on data stores of a plurality of security brokers;

generating a plurality of surrogate identifiers in the data stores of the security brokers, each surrogate identifier being associated with one user role;

associating users with user roles, each user being associated with one user role; and

determining access rights to the secured resources for each user according to a corresponding surrogate identifier without disclosing the corresponding surrogate identifier to the user, the corresponding surrogate identifier being associated with the user role of the user, determining access rights further comprising:

receiving a permissions request from a workstation and routing the permissions request to one of a plurality of security providers with one of the security brokers;

authenticating a computer user as a valid user with one of the security providers, wherein authenticating the computer user comprises:

invoking programatically an embedded component within the software application when a secured resource is accessed;

passing a resource name identifying the secured resource through the embedded component to a platform coordinator;

retrieving an identifier and a security provider name from the user via the platform coordinator;

passing the identifier and the security provider name to the security broker;

relaying the identifier to the security provider associated with the security provider name for authentication;

evaluating automatically the identifier against a data store the security provider;

returning an authentication result to the security broker;

storing an authentication token with a time stamp in a cache of the security broker when authentication is successful, the authentication token created by the security broker based on the authentication result;

retrieving the user role associated with the identifier from the data store of the security broker;

retrieving the surrogate identifier associated with the user role from the data store of the security broker;

passing the surrogate identifier and a secured resource name from the security broker to the security provider;

evaluating automatically the surrogate identifier against the data store of the security provider;

determining automatically permissions associated with the surrogate identifier on the security provider;

returning an authorization result associated with the surrogate identifier to the security broker;

creating automatically a permissions token on the security broker based on the authorization result;

relaying the permissions token to the platform coordinator, the permissions token comprising both the secured resource and access rights;

storing the permissions token with a time stamp in a cache on the platform coordinator; and

relaying the access rights to the software application through the embedded component; and

authorizing the user to access one of the secured resources with one of a plurality of security providers.

31. (New) A method for providing computer application security, the method comprising:

identifying secured resources within a software application;

grouping secured resources into user roles stored on data stores of a plurality of security brokers;

generating a plurality of surrogate identifiers in the data stores of the security brokers, each surrogate identifier being associated with one user role;

associating users with user roles, each user being associated with one user role; and

determining access rights to the secured resources for each user according to a corresponding surrogate identifier without disclosing the corresponding surrogate identifier to the user, the corresponding surrogate identifier being associated with the user role of the user, determining access rights further comprising:

receiving a permissions request from a workstation and routing the permissions request to one of a plurality of security providers with one of the security brokers;

authenticating a computer user as a valid user with one of the security providers; and

authorizing the user to access one of the secured resources with one of a plurality of security providers, wherein once the user is authenticated, authorizing the user comprises:

invoking programatically an embedded component within the software application when a secured resource is accessed;

passing a resource name identifying the secured resource through the embedded component to a platform coordinator;

retrieving an authentication token from a cache on the platform coordinator;

passing the authentication token and the resource name to the security broker;

comparing the authentication token against the cache on the security broker to identify a matching authentication token, the matching authentication token being associated in the cache with the surrogate identifier;

passing the surrogate identifier and the resource name from the security broker to the security provider;

evaluating automatically the surrogate identifier against the data store of the security provider;

determining automatically permissions associated with the surrogate identifier on the security provider;

returning an authorization result associated with the surrogate identifier to the security broker;

generating automatically a permissions token on the security broker based on the authorization result;

relaying the permissions token to the platform coordinator, the permissions token comprising both the secured resource and access rights;

storing the permissions token with a time stamp in a cache on the platform coordinator; and

relaying the access rights to the software application through the embedded component.

32. (New) A method for providing computer application security, the method comprising:

identifying secured resources within a software application;

grouping secured resources into user roles stored on data stores of a plurality of security brokers;

generating a plurality of surrogate identifiers in the data stores of the security brokers, each surrogate identifier being associated with one user role;

associating users with user roles, each user being associated with one user role;

determining access rights to the secured resources for each user according to a corresponding surrogate identifier without disclosing the corresponding surrogate identifier to the user, the corresponding surrogate identifier being associated with the user role of the user, determining access rights further comprising:

receiving a permissions request from a workstation and routing the permissions request to one of a plurality of security providers with one of the security brokers;

authenticating a computer user as a valid user with one of the security providers; and

authorizing the user to access one of the secured resources with one of a plurality of security providers; and

wherein determining access rights further comprises:

invoking programatically an embedded component within the software application when the secured resource is accessed;

passing a resource name identifying the secured resource through the embedded component to a platform coordinator;

retrieving an authentication token from a cache on the platform coordinator;

comparing the secured resource name with permissions tokens stored in the cache on the platform coordinator for a matching permissions token, the matching permissions token containing the secured resource name; and

relaying access rights associated with the matching permissions token to the software application through the embedded component.

33. (Currently amended) A method for providing computer security, the method comprising:

securing a plurality of resources within a software application;

identifying each of the plurality of resources in a data store;

selecting some of the plurality of resources;

grouping selected resources into user roles in the data store;

creating a plurality of user names and a plurality of aliases in the data store, each user name and each alias being associated with the same user role;

replicating the plurality of resources, the user roles, the plurality of user names and the plurality of aliases in a plurality of data stores; and

determining access privileges to the plurality of resources using an alias corresponding to a user name by virtue of the same one user role from one of the plurality of data stores, determining access privileges further comprising:

authenticating a user on the system with one of a plurality of security providers;

authorizing access rights to the secured resources in the software application with one of a plurality of security providers, wherein authorizing access rights comprises:

capturing a security call from the software application, the security call containing a name identifying a secured resource;

retrieving a user identifier;

passing the user identifier to a one of the security brokers;

retrieving one of the plurality of aliases from a data store of one of the security brokers, the retrieved alias corresponding to the user identifier;

passing the retrieved alias to a one of the security providers;

verifying the alias against one of the plurality of data stores on one of the plurality of security providers;

returning an encrypted permissions token to the software application; and

determining access rights to the secured resource according to the permissions token; and

receiving a permissions request from one of a plurality of workstations and routing the permissions request to one of the security providers with one of a plurality of security brokers.

34. (New) The method of claim 33, wherein retrieving a user identifier comprises:

gathering information about a user for authorizing access to secured resources, the information selected from the group consisting of user name and password, software token, hardware token, and digital signature.

35. (New) A process for authorizing access rights to secured resources in a software application, the process comprising:

authenticating a computer user to a computer security provider via a user identifier corresponding to the computer user, the computer security provider returning a result to a security broker according to the user identifier, the computer security provider being one of a plurality of security providers;

storing the result on the security broker;

retrieving a surrogate identifier from the security broker, the surrogate identifier corresponding to the result, the surrogate identifier being undisclosed to the computer user; and

authorizing the surrogate identifier to the computer security provider, the computer security provider returning surrogate permissions to the security broker, the surrogate permissions corresponding to the surrogate identifier, the surrogate permissions for determining access rights to secured resources in the software application according to the surrogate permissions, wherein authorizing the surrogate identifier to the computer security provider comprises:

passing the surrogate identifier to a security manager;

querying for the surrogate identifier in a permissions list on the security provider using the security manager;

determining surrogate permissions for the surrogate identifier according to the permissions list; and

returning the surrogate permissions to the security broker; and

wherein authorizing the surrogate identifier to the computer security provider further comprises:

passing the surrogate permissions from the security broker to a platform coordinator;

storing the surrogate permissions with a time stamp in a cache on the platform coordinator;

relaying the surrogate permissions to an embedded component within the software application;

passing the surrogate permissions to a function within the software application, the function capable of interpreting the surrogate permission; and

interpreting the surrogate permission using the function to permit or deny access rights to the secured resource.